Avertium & Appgate
ZERO TRUST NETWORK ACCESS

AVERTIUM®

www.avertium.com

877-707-7997

Company Overview

We are the cybersecurity services provider that companies turn to when they want more than standard security services. Every day, Avertium security experts rise to meet clients' not-so-standard business requirements, technology environments, processes and policies with a show-no-weakness approach to cybersecurity.

Unique Value Proposition

Comprehensive security and business approach to ZTN combining Appgate's best-in-class solution and the rigorous Avertium Engagement Methodology.

By the Numbers

☑ Gartner predicts by 2021, 60% of enterprises will phase out most VPNs in favor of ZTNA

☑ 78% of IT security teams are looking to embrace a zero-trust model in the near future

☑ Cyber threats are the #1 concern across all businesses, regardless of size

Disappearing perimeters, complex computing environments and data sprawl serve up vulnerabilities to would-be attackers whose efforts continue to gain momentum. Software defined perimeter (SDP) zero trust network access (ZTNA) establishes a dynamic digital identity-based perimeter to stop malicious traffic before it can even discover, let alone identify and target enterprise servers, cloud services or remote devices.

The Avertium show-no-weakness approach along with Appgate's SDP ZTNA solution creates the ideal combination for stopping bad actors in their tracks without requiring the rip and replace of expensive hardware typical of other solutions.

AVERTIUM BENEFITS

Avertium provides the heavy lifting for smooth implementation and administration of your ZTN deployment.

- Removes the complexity of enabling a zero trust architecture through a pragmatic, use-case driven approach

- Significantly strengthens defenses by eliminating "default trust"

- Drastically reduces the attack surface and eliminates lateral movement

- Integrates Network Access Control (NAC) feature to enforce device security through assessment prior to enabling access

- Powers up behavior-based threat detection and accelerates containment and incident response to the speed of automation

- Improves user experience for accessing many resources in multiple locations, even from different devices

- Identifies and organizes sensitive systems and data, and provides better understanding of how data is accessed

AVERTIUM ADVANTAGE

The rigorous **Avertium Engagement Methodology** sharpens focus by beginning with a pre-onboarding assessment to highlight the attack surface and define use cases and entitlement definitions to enable reducing the attack surface. Avertium then provides identity and access management integration and performs ongoing 24/7/365 platform management and support.
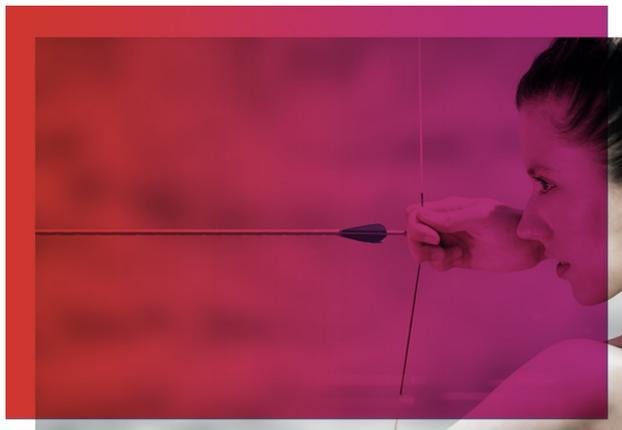
USE CASE	AVERTIUM
Company implemented split tunnel VPN to quickly move majority of the workforce to work-from-anywhere model, creating blind spots in user activity. Company would now need to scale VPN solution to adequately protect its environment, but does not have budget or resources.	ZTN contextually identifies the user to enforce identity –based policies and removes over-privileged access, replacing it with granular access control. ZTN is less cumbersome and expensive than VPN, and our SDP model requires limited network architecture and no new hardware to support it at scale.
Company is aware that perimeter-based security can allow a threat that breaches the exterior to run amok once inside the environment. Company is looking to improve its overall security posture, reduce its attack surface, and more easily fulfill compliance. Company lacks the time and/or expertise to implement ZTN, and is seeking partnership with a worthy service provider.	Avertium collaborates with you to fully assesses your access needs, beginning with an assessment to define the attack surface and appropriate entitlement definitions, establishes role-based data access needs, and classifies data and resources to provide valuable environment insight. This sets the path for implementing an effective ZTN architecture to improve overall security posture.
Company uses hybrid cloud environment, introducing complexity and inconsistency in the security environment. Company has limited insight into where all sensitive data flows and rests. Company may use a cloud access security broker (CASB) to manage identity and access.	ZTN integrates with existing security measures and automatically secures workloads, enforcing consistent controls regardless of data location or users. Our SDP ZTN approach is cloud agnostic and simplifies identity and access management while providing secure connectivity to all platforms.

AVERTIUM AND APPGATE

Avertium offers ZTN as a service (ZTNaaS) through its award-winning CyberOps Centers of Excellence, and blends Appgate's best-in-class technology with Avertium's cloud, networking and security expertise to bring the rigor of enterprise-level security to mid-sized and larger organizations challenged by the cybersecurity talent shortage, rapidly evolving threat landscape and budgetary constraints. Avertium's always-on turnkey zero trust offering removes the complexity of customer adoption, implementation and ongoing management.

avertium.com | 877-707-7997